AKSES JARAK JAUH LAYANAN INTRANET MELALUI LAYANAN VIRTUAL PRIVATE NETWORK

Akhmad Fauzi
Teknik Informatika, FTI, UPN "Veteran" Jawa Timur,
Email : masuzi@upnjatim.ac.id

INTISARI

Jaringan virtual yang Kumpulan beberapa komputer bahkan jutaan komputer, disebut dengan jaringan komputer bisa berupa jaringan lokal maupun interlokal, jaringan lokal atau disebut dengan LAN (Lokal Area Network) dan jaringan interlokal atau disebut dengan internet. Layanan internet merupakan fasilitas yang tidak akan bisa lepas dari kehidupan manusia sehingga diperlukan suatu cara untuk memanfaatkan internet dengan maksimal. Virtual Private Network (VPN) merupakan suatu cara untuk membuat sebuah jaringan bersifat "private" dan aman dengan menggunakan jaringan publik misalnya internet. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara point to point. Data dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi point to point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi private, data yang dikirimkan harus di enkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut "tunneling". Server yang berada dikantor bisa diakses melalui VPN dimanapun, kapanpun dengan aman, meskipun menggunakan infrastruktur jaringan internet dalam penggunaannya. Menurut pandangan user, kneksi VPN merupakan koneksi point to point antara user komputer dengan server korporasi dan data terkirim diatas jaringan "dedicated", padahal tidak demikian kenyataannya.

keywords : *Virtual Private Network, Jaringan komputer, Tunneling, Point to point*

PENDAHULUAN

Jaringan komputer merupakan bukan sesuatu yang baru untuk saat ini, seiring dengan perkembangan teknologi informasi yang melaju sangat pesatnya, jaringan komputer tidak akan lepas perannya didalam dunia teknologi informasi baik jaringan yang kecil maupun yang besar. Akses internet saat ini juga sudah menjadi kebutuhan rutin bagi hampir sebagian besar umat manusia. Tingginya tingkat kebutuhan akan informasi secara *virtual* dan elektronis serta akses internet ini mendorong kebutuhan akan *bandwidth* dan layanan yang lebih baik lagi dibandingkan yang sudah ada sekarang ini. Sehingga berusaha mencari layanan komunikasi yang handal, fleksibel, cepat, dengan harga yang murah untuk berbagai keperluan aplikasi yang mereka butuhkan.

Semakin besar jaringan komputer yang dibutuhkan maka semakin mahal infrastruktur yang dibutuhkan untuk dibangun, bisa dibayangkan jika pembangunan jaringan komputer dalam berbeda wilayah, untuk koneksinya harus bisa menghubungkan antara kota, atau wilayah yang berjauhan dengan kabel jaringan. Pembangunan jaringan komputer seperti itu akan sangat mahal sekali untuk saat ini harus bisa bagaimana caranya membangun infrastruktur jaringan yang menghubungkan antara wilayah yang berjauhan seperti antar kota, provinsi bahkan berbeda negara sekalipun. Pembangunan *Wide Area Network* menjadi tidak efektif lagi, untuk saat ini dibutuhkan bagaimana memanfaatkan jaringan public yang sudah ada yaitu jaringan internet yang bisa menghubungakan seluruh dunia. Pemanfaatan tersebut yaitu dengan membangun aplikasi *Virtual Private Network (VPN)* pemanfaatan jaringan internet dengan *VPN* merupakan jalan keluar dari kebutuhan jaringan komputer. Atas dasar itu maka penelitian ini akan membahas bagaimana akses jarak jauh dilakukan menggunakan *VPN.* Atas dasar uraian diatas maka dapat diketahui beberapa permasalahan yang sering dijumpai dalam pembangunan infrastruktur jaringan komputer, permasalahannya yaitu: bagaimana *VPN* memberikan manfaatnya dalam akses jarak jauh, terutama dalam fungsi sebagai administrator serta Masih mahalnya pembangunan infrastruktur jaringan komputer.

VPN (Virtual Private Network)

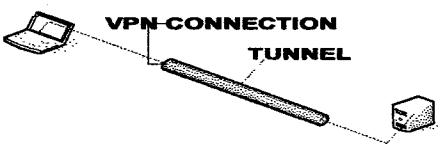
VPN (Virtual Private Network) merupakan suatu cara untuk membuat sebuah jaringan bersifat*"private"* dan aman dengan menggunakan jaringan publik misalnya internet. *VPN* dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung *point to point.* Data dienkapsulasi (dibungkus) dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-point* sehingga data dapat melewati jaringan pulik dan dapat mencapai tujuan.

Sedangkan untuk mendapatkan koneksi bersifat *private,* data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiahannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut *"tunneling".*

Kemampuan VPN

Beberapa kemampuan dari *virtual private network* yaitu a).Menyediakan keamanan "industrial-strength", b). Mengakomodasi komunitas pengguna yang berubah secara dinamis, c). Menyediakan kemampuan pertukaran informasi dalam berbagai bentuk form (web, file, dll), d) Mengakomodasi pengguna yang berbeda dengan berbagai macam browser, aplikasi, sistem operasi, dll, e) Memungkinkan pengguna masuk ke dalam grup atau administrator memasukkan identitas dalam sebuah cara yang dikendalikan tetapi mudah, f). Memelihara integritas sepanjang waktu, tanpa memperhatikan pergantian administrasi, perubahan teknologi, atau peningkatan kompleksitas sistem informasi perusahaan.

VPN-connection merupakan koneksi yang melewati *tunnel* yang sebelumnya telah dibuat oleh *VPN,*



Gambar 1: Koneksi secara *VPN*

Untuk mengakses kantor pusat bisa dilakukan dimana entah itu dirumah ataupun di jalan secara aman meskipun menggunakan infrastruktur jaringan internet dalam penggunaannya. Menurut pandangan *user,* koneksi *VPN* merupakan koneksi *point-point* antara *user* komputer dengan server korporasi dan data terkirim di atas jaringan *"dedicated"* padahal tidak demikian kenyataannya.

Perkembangan *VPN*

VPN dikembangakan untuk membangun sebuah intranet dengan jangkauan yang luas melalui jaringan internet. Intranet sudah menjadi komponen penting dalam suatu perguruan dewasa ini. Intranet dalam perusahaan akan berkembang sesuai dengan perkembangan perguruan tersebut. Dengan kata lain semakin besar perguruan tinggi maka akan semakin besar suatu perguruan tinggi maka intranet yang diperlukan juga semakin besar. Permasalahan ini akan semakin kompleks apabila perguruan tinggi tersebut mempunyai banyak cabang yang tersebar di berbagai kota dengan jarak yang jauh. Sedangkan di lain pihak seluruh cabang tersebut memerlukan suatu metode untuk selalu berhubungan, misalnya untuk tranfer dan sinkronisasi data.

Pada mulanya, sistem intranet deikembangkan dengan menggunakan sistem *dedicated line.* Sistem ini menawarkan kecepatan transfer data yang tinggi namun membutuhkan investasi yang mahal. Sistem ini tidak efektif untuk perguruan kelas menengah kebawah serta perguruan tinggi yang tersebar di berbagai wilayah dan saling berjauhan. Perkembangan internet yang cepat menawarkan solusi untuk membangun sebuah intranet menggunakan publik network (internet). Di lain pihak, kekuatan suatu industri juga berkembang dan menuntut terpenuhinya lima kebutuhan dalam internet, yaitu:

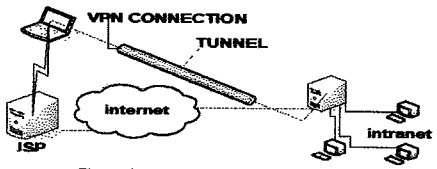
a) **Kerahasian,** dengan kemampuan *scramble* atau *encrypt* pesan sepanjang jaringan yang tidak aman,
b) **Kendali akses,** menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima,
c) ***Authentication,*** *yaitu menguji identitas dari dua perguruan tinggi yang* mengadakan transaksi,
d) **Integritas,** menjamin bahwa file atau pesan tidak berubah dalam perjalanan,

e) *Non-repudiation,* yaitu mencegah dua perguruan tinggi saling menyangkal bahwa mereka telah mengirim atau menerima sebuah file.

Berikut adalah beberapa kriteria yang harus dipenuhi oleh *VPN* dalam menjawab tantangan globalisasi tersebut antara lain : *User Authentication, Address Management, Data Encryption, Key Management, Multiprotocol Support.*

Aplikasi *VPN*

Konfigurasi *VPN* umumnya digunakan untuk *Remote Acces Over Internet.* Gambar berikut ini menunjukan sebuah teknik untuk seorang *user* untuk berhubungan secara *remote* dengan jaringan lokal.



Gambar 2: Koneksi *VPN*

Seorang klien cukup berhubungan dengan *ISP (Internet Service Provider)* lokal lalu *software VPN* akan membuat jaringan khusus secara maya antara *dial-up user* dengan server jaringan lokal melalui internet.

Protokol-Protokol *VPN*

Beberapa protocol yang digunakan untuk mengembangkan *Virtual Private Network* adalah sebagai berikut : a). *PPTP* ***(Point to Point Tunneling Protocol), b). L2TP (Layer Two Tunneling Protocol), c) IPSEC (Internet Protocol Security, d). PPTP Over L2PT, e). IP-IN-IP***

ANALISA DAN PERANCANGAN SISTEM

Analisa Sistem

Pada banyak organisasi besar, organisasi tersebut memiliki kantor-kantor cabang yang tersebar di banyak tempat. Kantor cabang-kantor cabang tersebut tentu memiliki kebutuhan untuk saling berhubungan satu sama lainnya. Pada masa-masa awal jaringan komputer, solusi yang biasa digunakan adalah dengan membangun jaringan private yang menghubungkan seluruh kantor cabang yang ada atau yang biasa disebut dengan *Wide Area Network (WAN).* Dengan berkembangnya jaringan publik atau biasa disebut dengan internet, solusi dengan membangun *WAN* menjadi solusi yang sangat mahal dan tidak fleksibel. Dengan berkembangnya *Virtual Private Network* (*VPN*), sebuah organisasi dapat membangun jaringan *private* maya diatas jaringan publik untuk menghubungkan seluruh kantor cabang yang dimilikinya.

a) Kendali akses, menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

b) Kerahasian, dengan kemampuan *scramble* atau *encrypt* pesan sepanjang jaringan yang tidak aman,
c) *Authentication,* yaitu menguji identitas dari dua lembaga yang mengadakan transaksi,
d) Integritas, menjamin bahwa file atau pesan tidak berubah dalam perjalanan,
e) *Non-repudiation,* yaitu mencegah dua perguruan tinggi saling menyangkal bahwa mereka telah mengirim atau menerima sebuah file.

Perancangan Sistem

Perancangan sistem disini adalah suatu perancangan pembangunan *VPN,* dimulai dari awal pembangunan sampai simulasi pembangunan *VPN* dimana didalamnya terdapat kebutuhan sistem, simulasi jaringan *VPN,* deskripsi sistem dan *flow chart.*

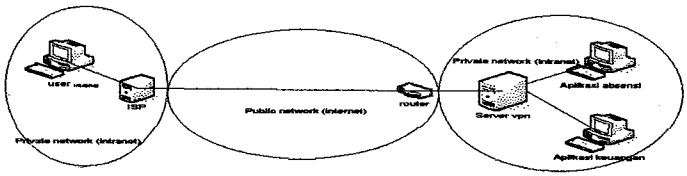
Kebutuhan sistem

Kebutuhan sistem dalam pembangunan *virtual private network* tidak harus mempunyai spesifikasi tinggi, karena dalam pembangunannya kebutuhan yang paling penting adalah sebuah sistem operasi yang bisa membangun *VPN,* sistem operasi yang dipilih adalah linux debian yang gratis sehingga kebutuhan lebih ditekankan pada alat-alat apa aja yang dibutuhkan, *sistem debian* dikenal karena kehandalan dan kestabilan paket sistemnya, *software-software* yang di realese dalam *stable branch* oleh debian telah melalui pengujian ketat oleh ribuan programmer seluruh dunia.

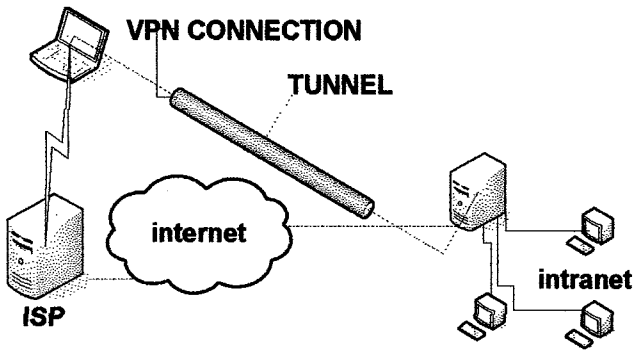
Simulasi Jaringan *VPN*

Infrastruktur *Virtual Private Network* dilakukan dengan simulasi di ruangan Komunitas Linux UPN. Simulasi di bangun dengan mensimulasikan jaringan lokal dan jaringan interlokal atau disebut juga jaringan intranet dan jaringan internet.

Simulasi jaringan *VPN* ini dibangun secara maksimal, untuk membuat tiruan dari *virtual private network,* sehingga apa yang dilakukan dalam simulasi ini merupakan bentuk duplikasi dari kenyataannya, yaitu pembangunan *virtual private network.* Dalam simulasi membutuhkan 6 buah PC untuk dijadikan sebagai : Komputer aplikasi 1, Komputer aplikasi 2, *VPN* server, Router, *ISP (Internet ServiceProvider),* Komputer klien.



Gambar 3 : Simulasi *VPN*



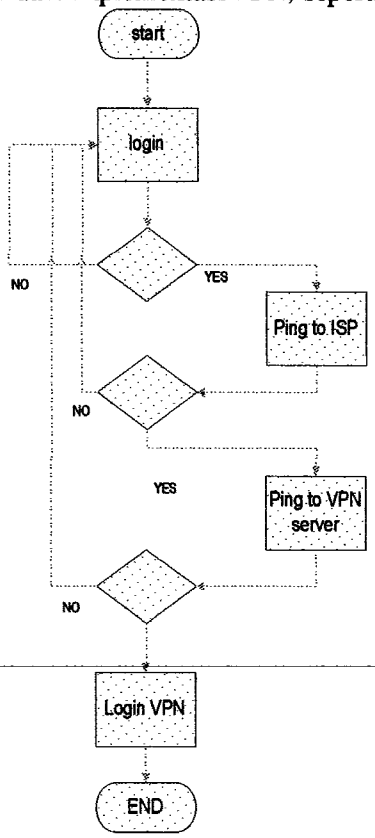
Gambar 4: Koneksi *VPN*

a) Komputer klien adalah komputer yang dijalankan oleh klien yang mengakses komputer yang ada di server *VPN* dengan tujuan untuk *maintenance*. Komputer klien mengakses bisa dimana-mana bahkan *mobile*, klien mengakses jaringan public dengan menggunakan *tunneling* untuk keamanannya.
b) *ISP (Internet Service Provider)* atau disebut juga sebagai penyedia jasa internet
c) Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain. Proses routing dilakukan secara hop by hop. IP tidak megnetahui jalur keseluruhan menuju tuuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang menurutnya lebih dekat ke host tujuan. Router dapat digunakan untuk menghubungkan sejumlah LAN sehingga trafik yang dibangkitkan oleh suatu LAN terisolasikan dengan baik dari trafik yang dibangkitkan oleh LAN yang lain. Jika dua atau lebih LAN terhubung dengan router, setiap LAN dianggap sebagai subnetwork yang berbeda. Merip dengan bridge, router da[at dihubungkan network interface yang berbeda. Router terletak pada Layer 3 dalam OSI, router hanya perlu mengetahui Net-Id (no mor jaringan) dari data yang diterimanya untuk diteruskan ke jaringan yang dituju. Cara kerjanya setiap paket data yang datang, paket data tersebut dibuka lalu dibaca header paket datanya kemudian mencocokan atau membandingkan ke dalam table yang ada pada routing jaringan dan diteruskan ke jaringan yang dituju melalui suatu interface. Untuk mengetahui network mana yang akan dilewatkan router akan menambahkan (Logical AND) Subnet Mask dengan paket data tersebut.
d) Server *VPN* yaitu sebuah komputer yang berfungsi untuk memanajemen seluruh klien.

e) *TUNNEL* merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan data secara terselubung. Disebut *Tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua *endpoint* atau ujung, sehingga paket yang lewat pada *tunnel* hanya akan melakukan satu kali lompatan atau *hop.* Data yang akan ditransfer dapat berupa *frame* (paket) dari protokol yang lain.

Flow Chart

Berikut merupakan *flow chart* dari implementasi *VPN,* seperti dibawah ini



Gambar 5 : *Flow chart VPN*

Deskripsi Sistem

Virtual Private Network VPN merupakan suatu cara untuk membuat sebuah jaringan bersifat*"private"* dan aman dengan menggunakan jaringan publik misalnya internet. *VPN* dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung *point to point.* Data dienkapsulasi (dibungkus) dengan *header* yang berisi informasi *routing* untuk mendapatkan koneksi *point-point* sehingga data dapat melewati jaringan pulik dan dapat mencapai tujuan.

VPN akan menjadi solusi pada waktu koneksi *Wide Area Network (WAN)* sangat rumit di implementasikan. Kebingungan akan bertambah jika sistem yang dikehendaki meliputi banyak kepentingan. Sentralisasi data, *maintenance,* remote sistem dan masih banyak lagi kebutuhan sejalan dengan perkembangan teknologi informasi

a).Mengggunakan *VPN* lebih Murah

Perbandingan biaya pembangunan antara *Area Network (WAN),* dengan *VPN,* sangat jauh perbedaannya dari pada membangun jaringan baru. contoh: jika UPN, akan membangun jaringan *Wide Area Network* untuk menyatukan ketiga UPN yang tersebar di Jakarta, Yogyakarta dan Surabaya, akan menyedot biaya yang sangat besar (sumber harga: A Mohammad BS, tgl 15 Mei 2007).

Tabel 1: Prakiraan biaya jaringan *WAN*

Jarak UPN	Fiber Optik	Biaya	Keterangan
Jakarta – Yogyakarta 500 km	550 km	Rp.11.000.000.000	harga 20.000 per meter
Yogyakarta – Surabaya 350 km	400 km	Rp.8,000,000,000	harga 20.000 per meter

Wide Area Network adalah konsep jaringan yang sangat mahal untuk diaplikasikan pada sistem jaringan komplek, berapa nilai investasi yang harus dikeluarkan, apalagi jika mempunyai banyak cabang tersebar keseluruh propinsi dan harus menyiapkan perangkat keras untuk setiap lokasinya.

b). Mengggunakan *VPN* Terjamin Keamanannya

Akses internet atau jaringan publik sangat beresiko sekali ketika ada pengiriman data-data penting, internet merupakan jaringan publik dimana semua orang yang ada di dunia ini bisa mengaksesnya, *VPN* menawarkan konsep yang berhubungan dengan keamanan pengiriman data.

Komunikasi yang memanfaatkan PPTP dapat dijamin lebih aman, mengapa demikian ? Otentifikasi pemakai jaringan dilakukan dengan menggunakan protocol otentifikasi yang ada di dalam Windows NT Remote Access Service (RAS) – PAP dan CHAP. MS-CHAP mendukung hash MD4 serta DES yang digunakan di LAN Manager. Otentifikasi tambahan dapat dilakukan oleh ISP pada ujung hubungan antara pemakai dengan ISP jika dibutuhkan. Enkripsi data dilakukan dengan menggunakan protocol enkripsi RAS-RSA RC4. Dengan menggunakan Microsoft Remote Access Services (RAS) maka kita dapat menurunkan waktu kompresi, enkripsi dan integrasi kedalam model administrasi Windows NT. PPTP juga menggunakan fasilitas keamanan yang disediakan oleh PPP, MS-CHAP (PPP authentication) dan digunakan untuk mevalidasi data-data pemakai dalam domain di Windows NT. Hasilnya adalah *session key* yang digunakan untuk mengenkripsi data pemakai. Selain itu Microsoft mengimplementasikan

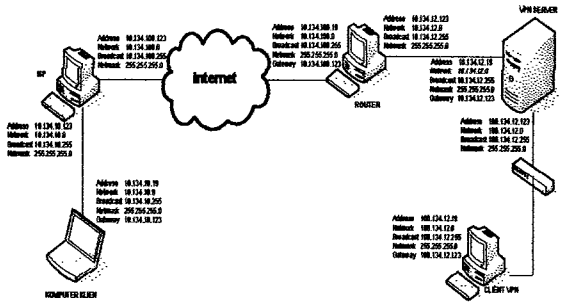
CCP (*Compression Control Protocol*) yang memiliki bit untuk negoisasi enkripsi. RAS client dapat diatur untuk hanya melakukan koneksi dengan mode terenkripsi, sementara itu RAS server juga dapat dikonfigurasi untuk hanya menerima koneksi dengan RAS yang terenkripsi.

IMPLEMENTASI *VIRTUAL PRIVATE NETWORK*

Implementasi dari *VPN* merupakan proses pembangunan jaringan *Virtual Private network,* jaringan ini dibangun dengan mensimulasikan lima buah komputer.

Simulasi Koneksi *VPN* di Ruangan KoLu

Kebutuhan komputer untuk membangun jaringan ini dibutuhkan enam buah kmputer antara lain digunakan untuk : *VPN* server, Router, *ISP (Internet ServiceProvider),* Komputer klien, Komputer aplikasi 2, Switch



Gambar 5 : *Jaringan VPN Uji Coba di KULO*

Komputer *VPN* Server

Komputer server ini menggunakan sistem operasi Linux *distro debian etch.* Supaya server bisa berkomunikasi dengan berbagai klien maka di server di install *PPTP* sebagai produk yang dikembangkan Microsoft sehingga server bisa berhubungan dengan klien meskipun memakai sistem operasi Microsoft . Pastikan paket ppp sudah terinstall sebelumnya: Untuk instalasi, paket bisa diambil di mirror *kambing.org* atau ditempat lainnya yang menyediakan paket *debian etch.* Jurusan Teknik Informatika sudah menyediakan mirror *debian etch* dengan alamat *deb* http://10.134.11.11/debian *etch main contrib non-free,* maka bisa langsung diarahkan ke mirror tersebut.

Proses instalasi server

- rubah alamat yang berada di `/etc/apt/sources.list` dengan perintah
  `#nano /etc/apt/sources.list`
  tambahkan `deb http://10.134.11.11/debian etch main contrib non-free` pada file sources.list tersebut.
- pastikan ppp sudah terinstal di seinrver cari dengan perintah
  `#dpkg -l | grep ppp`

```
ii kppp 3.5.5-5 modem dialer and ppp frontend for
KDE
ii ppp 2.4.4rel-8 Point-to-Point Protocol (PPP)
daemon
```

- install pptpd sebagai daemon untuk *VPN* dengan protocol *PPTP*.

```
#apt-get install pptpd
```

- konfigurasi file /etc/pptpd.conf

Konfigurasi pada /etc/pptpd.conf berisi konfigurasi standart PoPToP, sedangkan detail konfigurasi terdapat /etc/ppp/options.

```
#nano /etc/pptpd.conf
```

- Konfigurasi file /etc/ppp/options-pptpd

```
#nano /etc/ppp/options-pptpd
==============================
name*
lock
mtu 1450
mru 1450
proxyarp
auth
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 3
lcp-echo-interval 5
deflate 0
#metode authentikasi yang diinginkan
+chap
+mschap-v2
=======================================
```

Metode authentikasi disesuaikan dengan kebutuhan. Dalam hal ini menggunakan *chap* dan *mschap-v2* (untuk klien windows).

- Konfigurasi fille /etc/ppp/chap-secrets

```
#nano /etc/ppp/chap-secrets
=======================================
#secret for authentication using CHAP
#Client   Server      Password    IPAddress
kolu            *     kolujuga    *
cyberedu  *           cyberedu    *
hima            *     himatifa    *
=======================================
```

- Restart service

```
#/etc/init.d/pptpd restart
```

Komputer *Router (ISP)*

a) Komputer *Router 1 (ISP 1)*

Router disini merupakan sebuah PC yang di setting mempunyai fungsi sebagai *Router, Router* ini berfungsi sebagai ISP 1 menggunakan sistem

operasi linux *ubuntu 6.10 edgy,* mempunyai dua *lancard* yang disetting menjadi eth0 dan eth1.

```
#nano /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
        address 11.134.11.199
        network 11.134.11.0
        broadcast 11.134.11.255
        netmask 255.255.255.0
        dns-nameservers 192.168.0.252
auto eth1
iface eth1 inet static
        address 100.200.100.254
        network 100.200.100.0
        broadcast 100.200.100.255
        netmask 255.255.255.0
        dns-nameservers 192.168.0.252
```

b) Komputer *Router (ISP 2)*

```
#nano /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
        address 100.200.100.253
        network 100.200.100.0
        broadcast 100.200.100.255
        netmask 255.255.255.0
auto eth1
iface eth1 inet static
        address 100.100.200.254
        network 100.100.200.0
        broadcast 100.100.200.255
        netmask 255.255.255.0
        dns-nameservers 192.168.0.252
```

Komputer *VPN client*

Dibawah ini menggunakan contoh 2 macam sistem operasi yaitu, sistem operasi linux dan Microsoft Windows XP.

Menggunakan *Windows XP*

Client menggunakan sistem operasi *Microsoft Windows* yang support terhadap *PPTP.*

- Klik next
- Pilih *connect to the network at my workplace,* klik next
- Pilih *virtual private network connection,* klik next
- Tuliskan nama perusahaan, klik next

- Pilih *do not dial the initial connection,* klik next
- Inputkan IP address *VPN* server sebagai tujuan dari client ke server. Ddalam hal ini IP address server adalah 10.134.11.199, klik next
- Instalasi *VPN client* lewat wizard telah selesai dilakukan, klik finish untuk mengakhiri konfigurasi
- Klik kanan properties, informasi mengenai security
- Konfigurasi client disesuaikan dengan konfigurasi server dengan memakai *Microsoft CHAP Version 2 (MS CHAP v2)*
- Mengakses *VPN,* masukan username serta password

a) *Client* sistem operasi Linux

Sebagai contoh client sistem operasi linux menggunakan linux distro Ubuntu 6.10, sebelumnya install dulu kvpnc, kvpnc merupakan aplikasi *VPN* client yang tersedia untuk linux. Cek aplikasi *kvpnc* sudah tersedia apa belum,

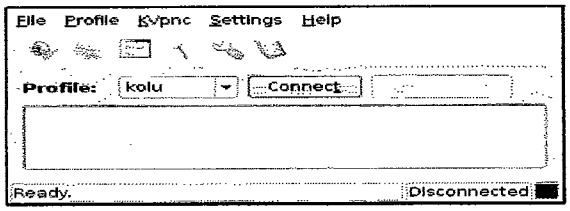
#dpkg -l | grep kvpnc

jika belum tersedia install dengan perintah

#apt-get install | kvpnc

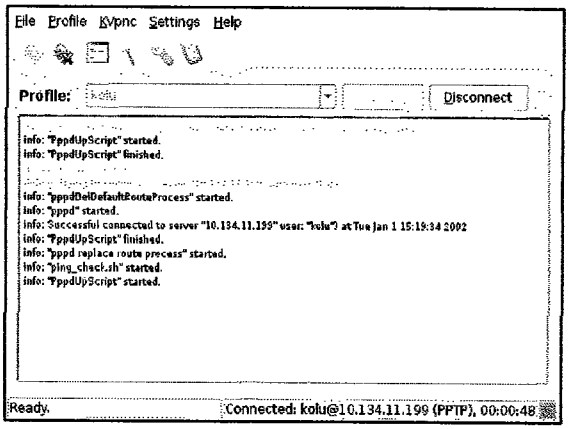
proses instalasi sudah selesai maka buka aplikasi *kvpnc*

- Buka profil pilih new profile (wizard)



Gambar 7 : Tampilan awal *kvpnc*

- Pilih next
- Pilih *Microsoft PPTP,* klik next
- Pilih require MPPE, klik next
- Masukan Username dan Password sesuai yang diberikan oleh server, klik next
- Pilih lancard yang digunakan eth0, klik next
- Isi *profile name :* hima, *Description* : himatifa ok, *VPN gateway* : 10.134.11.199, *VPN gateway* merupakan IP dari server *VPN,* klik next
- Finish
- *Profile*: Pilih hima, klik *connect*
- *Client* terhubung dengan server *VPN*



Gambar 8: *Connected Client*

b) Komputer *Router (ISP 1)*

Router disini merupakan sebuah PC yang di setting mempunyai fungsi sebagai *Router, Router* ini berfungsi sebagai ISP 1 menggunakan sistem operasi linux *ubuntu 6.10 edgy,* mempunyai dua *lancard* yang disetting menjadi eth0 dan eth1.

```
#nano /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
        address 11.134.11.199
        network 11.134.11.0
        broadcast 11.134.11.255
        netmask 255.255.255.0
        dns-nameservers 192.168.0.252

auto eth1
iface eth1 inet static
        address 100.200.100.254
        network 100.200.100.0
        broadcast 100.200.100.255
        netmask 255.255.255.0
        dns-nameservers 192.168.0.252
```

KESIMPULAN

Meskipun jaringan yang dibuat merupakan jaringan simulasi dari jaringan *Virtual Private Network* yang sebenarnya, akan tetapi dari hasil simulasi tersebut dapat disimpulkan :

Alasan jarak, tidak akan menjadi masalah lagi karena selama terkoneksi dengan internet, *VPN* bisa digunakan. Keamanan yang terjamin, dengan *VPN* keamanan akan terjamin seperti jaringan pribadi karena di *VPN* ada proses enkapsulasi, sehingga pengiriman data aman. Penggunaan infrastruktur berlebihan tidak akan terjadi, contoh tidak perlu membuat jaringan pribadi antara 3 UPN yang tersebar di Surabaya, Yogyakarta dan Jakarta.

Virtual Private Network (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh *(access remote)* menggunakan jaringan internet untuk akses *Lokal Area Network.* Penggunaan *VPN* akan menjadi sangat populer saat ini karena *VPN* memberikan jaminan keamanan dan reliabilitas yang hampir sama dengan jaringan pribadi. *VPN* sangat mudah digunakan, dengan menginstalasikan *VPN client* pada komputer atau laptop pemakai, maka pemakai dapat akses ke *Lokal Area Network* dengan fasilitas *VPN* lewat jaringan internet

DAFTAR PUSTAKA

Aris Wendy Sunyoto (2006). VPN Sebuah Konsep , Teori dan Implementasi. Penerbit BukuWeb.com, Surabaya

http://soedirman.gudangupload.com/obj/3c492aabb6533f07d9485b797dcc4747/45f29e9a/aldedi/ipsec-dedi.pdf, instalasi dan Konfigurasi VPN IPsec, tanggal 23 Mei 2007

http://ikc.cbn.net.id/populer/tommy-vpn.php, *Virtual Private Network (VPN) Dynamic.* Tanggal 12 Pebruari 2007.